WASHINGTON, DC –On Friday, Congressman Joe Sestak (PA-07) voted to support the FISA Amendments Act of 2008 (H.R. 6304) to update the Foreign Intelligence Surveillance Act (FISA) which was originally passed in 1978. This new bill, the result of strong bipartisan efforts, improves our nation's security by ensuring that there is no gap in intelligence collection against terrorists, while protecting our civil liberties by preventing the government from eavesdropping on American citizens without a warrant. It also provides for court review of liability for telecommunications companies, increases oversight of intelligence activities, and clarifies that the FISA Act and Title III of the Criminal Code are the exclusive means by which the Government may conduct surveillance on U.S. soil. As a result, this bill goes further to protect American civil liberties than either the Senate Bill which had been under discussion, or the original FISA Act. The bill passed the House with a vote of 293 – 129. —

"I support the revised FISA legislation today because it finds the right balance between two critical objectives. It allows the intelligence community to effectively conduct surveillance activities and gather intelligence information while protecting the privacy of the American people," said Congressman Sestak. "The legislation will establish the correct procedures that must be followed going forward to ensure protection of American civil liberties. It also provides oversight of government powers and holds accountable an Administration that has eroded American civil liberties that I spent 31 years in the Navy fighting to preserve."

First and foremost, Congressman Sestak believes that ensuring national security for the American people is the number one responsibility of Congress and the President. This new FISA bill approved by the House bill does that. It ensures that during an emergency, wiretapping can be conducted immediately on any terrorist threat even without a FISA court warrant and allows surveillance for up to seven days before the FISA court must be notified. In addition, the House Bill includes proliferators of weapons of mass destruction (WMD) in the scope of coverage – which were not included in the original FISA Act or the Senate bill. So, this new bill broadens and enhances the present surveillance authority ongoing and in an emergency situation.

Second, contrary to the Senate bill, the House FISA bill provides for proper oversight and review of the procedures to be followed in the surveillance program—which has been lacking under the current Administration over the past six years. The new House bill helps streamline the warrant obtaining process and strengthens intelligence gathering while also including safeguards to ensure that FISA procedures are being followed correctly. This includes mandatory reviews conducted by the Inspector General and semi-annual reports to House and Senate Intelligence and Judiciary Committees. So, the new House bill provides improved protection of American civil liberties while streamlining the authorization process.

Third, the new bill provides standards and procedures for determining liability for electronic communication service providers who assisted the Government. This provides for meaningful review by the District Court of the Attorney General's certification attesting that the liability protection standard had been met and supported by substantial evidence. The plaintiffs and defendants have the opportunity to file public briefs on legal issues. Congressman Sestak has been actively opposed to immunity for telecommunication companies. So, a secure review of telecommunication company actions can take place in the Courts – the proper branch of the government charged with adjudicating compliance with existing laws.

As important, there is no immunity provided for any actions against government for any alleged injuries caused by government officials. There is a requirement for the Inspectors General (IG) of Department of Justice, Department of National Intelligence, National Security Agency, and Department of Defense to conduct a comprehensive review of the President's warrantless surveillance program and provide those reviews to the Intelligence and Judiciary Committees. This report will review all of the facts necessary to describe the establishment, implementation, product, and use of the program, as well as communications with, and participation of, individuals and entities in the private sector related to the program. As a result, there will be accountability if abuses are found to have occurred.

To expand on the key points above:

PRIVACY AND CIVIL LIBERTY PROTECTIONS FOR AMERICANS

Exclusivity. The Act strengthens the requirement that FISA and specific chapters of Title 18 are the exclusive means by which electronic surveillance and certain criminal law interceptions may be conducted. In addition to the statutes specifically listed in the exclusivity provision, the Act provides that only an express statutory authorization for electronic surveillance or interception may constitute an additional exclusive means for that surveillance or interception.

Targeting Procedures. Knowing if a target is outside the U.S. is key to the protection of Americans. At least annually, the AG and DNI must submit to the FISA Court for review and approval targeting procedures for making that fundamental determination which governs collection under this bill.

Minimization Procedures. Making sure that information that is acquired about Americans, in the course of targeting foreigners, is used only for proper intelligence or law enforcement purposes is a second line of defense for Americans. These procedures must be reviewed and approved at least annually by the FISA Court.

Individual Judicial Orders for Surveillance of Americans. The Act requires individual FISA Court orders based on probable cause for the targeting of Americans not only when they are within the U.S. but also, for the first time, when they are outside of the United States -- whether they

are working, studying, or traveling abroad.
Reverse Targeting Guidelines. The Act requires adoption by the Attorney General and submission to the Congress and FISA Court of guidelines to ensure compliance with the Act's limitations, including its prohibition on reverse targeting.

TIMING OF COLLECTION AND JUDICIAL REVIEW
Timing of Judicial Review. The Act requires that the targeting procedures shall be submitted to and approved by the FISA court before the collection begins.
Exigent Circumstances. In rare cases, collection can begin while the court considers authorization only if the AG and DNI certify to the court that exigent circumstances exist and critical intelligence could be lost. The AG and DNI must submit procedures within 7 days and the court would make a determination within 30 days. During this period, all relevant minimization and reverse targeting guidelines would apply.

LIABILITY PROTECTIONS AND OBLIGATIONS OF AMERICAN COMPANIES
Prospective Immunity. The Act ensures that the cooperation shall be in accordance with law, by providing an opportunity for the companies to challenge in court the lawfulness of directives to them and for the Government to compel compliance through judicial proceedings. Companies that act in accordance with directives provided under the law shall be protected against future liability.
Retroactive Immunity. The Act provides standards and procedures for liability protection for electronic communication service providers who assisted the Government between September 11, 2001 and January 17, 2007, when the surveillance program was brought under the FISA Court. A district court hearing a case against a provider will decide whether the Attorney General's certification attesting that the liability protection standard has been met and is supported by substantial evidence. In making that determination, the court will have the opportunity to examine the highly classified letters to the providers that indicated the President had authorized the activity and that it had been determined to be lawful. The plaintiffs and defendants will have the opportunity to file public briefs on legal issues and the court should include in any public order a description of the legal standards that govern the order. The immunity provision of the Act does not apply to any actions against the Government for any alleged injuries caused by government officials. Nor does the immunity provision involve any statement by the
Congress, pro or con, on the legality of the President's program.

OVERSIGHT AND ACCOUNTABILITY
Inspector General Review. The Act directs the Inspectors General of the Department of Justice, the Office of the DNI, the National Security Agency, and the Department of Defense to complete a comprehensive review, within the oversight authority of each IG, of the President's Surveillance Program. In no later than a year, the Inspectors General shall submit a report to

Congress; the report shall be unclassified but may include a classified annex. The IG review will be an especially important vehicle for reporting to Congress on the facts of the President's program, as well as to the public, to the extent classification permits.
Multiple Levels of Oversight. The Act provides for multiple levels of oversight both within the Executive Branch, including by Department of Justice and Intelligence Community Inspectors General, and in regular reporting to both the Congress and the FISA Court.
Sunset. The Act will sunset at the end of 2012 ensuring that the next Administration, together with the Congress, will address whether the Act should be made permanent or modified based on experience.

"As Director of the Navy's anti-terrorism unit after 9/11, I saw the value of data-mining facilitated by proper eavesdropping. I also understand the FISA system and its role in the proper balance of civil liberties with national security needs. I believe strongly that this bill enhances our intelligence gathering capability and better protects both the American people and their civil liberties as written in our Constitution," added the Congressman.

Born and raised in Delaware County, former 3-star Admiral Joe Sestak served in the Navy for 31 years and now serves as the Representative from the 7th District of Pennsylvania. He led a series of operational commands at sea, including Commander of an aircraft carrier battle group of 30 U.S. and allied ships with over 15,000 sailors and 100 aircraft that conducted operations in Afghanistan and Iraq. After 9/11, Joe was the first Director of "Deep Blue," the Navy's anti-terrorism unit that established strategic and operations policies for the "Global War on Terrorism." He served as President Clinton's Director for Defense Policy at the National Security Council in the White House, and holds a Ph.D. in Political Economy and Government from Harvard University. According to the office of the House Historian, Joe is the highest-ranking former military officer ever elected to the U.S. Congress.

###